



Windows NT 4.0 Workstation Security Assessment Guide

July 9, 2001

Prepared by:
Barre Bull, Sr. IT Security Analyst
Don Truax, HW/SW Installation Tech



1953 Gallows Rd., 2nd Floor
Vienna, VA 22182

SAIC-6099-2001-222

Prepared for:
Mr. Greg Montgomery
U.S. Department of Agriculture
Room 431-W
Whitten Building
14th and Independence
Washington, D.C. 20250

FOR OFFICIAL USE ONLY

U.S. Department of Agriculture

Washington, D.C. 20250

USDA Windows NT Workstation Security Assessment Guide

1. PURPOSE

This Security Assessment Guide is designed to assist Agency ISSPMs in satisfying their responsibility to develop and implement a comprehensive risk management program as defined in DR 3140-001, "USDA Information Systems Security Policy." By using this guide, Agency ISSPMs can identify areas where Department Information Security requirements are not being met and develop an action plan to ensure all security requirements are satisfied.

2. SCOPE

This guide is to be used by all USDA organizational elements to help assess the security posture of Windows NT 4.0 Workstations. This checklist is ***not intended to be a configuration guide*** but a tool to assist in determining if the system meets the requirements for a Sensitive But Unclassified (SBU) system and assessing the vulnerabilities, both current and potential, of the system. The checks performed are based on Federal, USDA, and Best Security Practices for the protection of SBU data. This checklist does not address applications that may be installed on the system or special purpose configurations (i.e. web servers, database servers, etc.).

3. BACKGROUND

Risk Assessments are mandated by OMB Circular A-130, Appendix III, "Security of Federal Automated Information Resources." A security risk assessment process is a comprehensive evaluation of the system's technical and non-technical security features. It establishes the extent that a specific design and implementation meets specific security requirements. USDA does not currently have a comprehensive security risk assessment process. This guide is intended to serve as an interim measure, until formal risk assessment policies and procedures can be developed and implemented.

4. REFERENCES

a. External

- (1) Public Law 100-235, "Computer Security Act of 1987"
- (2) Public Law 93-579, "Privacy Act of 1974"
- (3) Public Law 93-502, "Freedom of Information Act"
- (4) Public Law 99-474, "Computer Fraud and Abuse Act"
- (5) OMB Circular No. A-130 Appendix III, "Security of Federal Automated Information Resources," revised February 8, 1996.
- (6) OMB Circular No. A-123, "Management Accountability and Control," June 29, 1995.

b. USDA Internal Regulations

- (1) DR 3140-001, "USDA Information Systems Security Policy" dated may 15, 1996
- (2) DM 3140-1 "USDA Management ADP Security Manual" dated March 5, 1992

Windows NT Workstation Assessment Guide

This assessment should be completed by the Agency's ISSPM or designated alternate in conjunction with the Agency Assessment Checklist. Answer all questions. Provide supplemental information as appropriate. All "No" answers must include supplemental information (such as the given reason why the requirement cannot be met) and an action plan that describes how the requirement will be met, as well as a schedule for completion of the plan. Typically, this would be done by developing the action plan in this document and reflecting this in the security plan for the agency.

Agency/System Identification:

Agency (Agency, Office, Bureau, Service, etc.):	
Address	
Date of last Assessment:	

Test Number: 1	SITE:	DATE:	TIME:
Test Name: NT Workstation Access and Configuration			
Resources Required:	Access to an NT Workstation, Valid user account. (Either a domain account or workstation account depending on how system is configured.)		
Personnel Required:	NT Workstation Administrator.		
Objectives:	To determine that the NT Workstations are configured to meet USDA requirements pertaining to systems protection, user access privileges and virus protection.		
Procedure Description: (Summary)	Verify that access is properly controlled, virus protection software is installed, configured and functioning properly,. Verify version and service pack level of operating system.		

Detailed Procedures and Results

Step #	Procedure Description	Expected Results	Actual Results (If different from Expected)	Y/N/P
1.	Ask the System Administrator if the hard drive is formatted using NTFS.	Hard drive is formatted using NTFS.		
2.	Ask the System Administrator if there is an Emergency Repair Disk for the system.	There is an Emergency Repair Disk for the system.		
3.	Ask the System Administrator if the Emergency Repair Disk is stored in a secure environment.	The Emergency Repair Disk is stored in a secure environment.		
4.	Observe that the system to be assessed is locked or that a password protected screensaver has been implemented.	System is locked or a password-protected screensaver is active.		
5.	Ask the System Administrator if the CMOS on all workstations are password protected.	The CMOS on all workstations are password protected.		
6.	Ask the System Administrator if the workstation CMOS has been configured to boot only from the hard drive.	The workstation CMOS has been configured to boot only from the hard drive.		
7.	Use the Secure Attention Sequence (Ctrl+Alt+Delete) to access the workstation logon screen.	Logon screen appears.		
8.	Verify that a Legal Notice dialog box appears prior to the Logon dialog box.	A Legal Notice dialog box appears prior to the Logon dialog box.		

Step #	Procedure Description	Expected Results	Actual Results (If different from Expected)	Y/N/P
9.	Click the OK button in the Legal Notice dialog and continue with log on.	Logon Dialog window is presented on screen.		
10.	Verify that there is no User ID from a previous session in the User ID portion of the logon window.	There is no User ID from a previous session in the User ID portion of the logon window.		
11.	Observe how many buttons are at the bottom of the logon window.	3 buttons are on the logon window, the Logon button, the Cancel button and the Help Button. The Shutdown button has been disabled (grayed out).		
12.	Ask the SA if the Guest account has a password.	Guest account has a password.		
13.	Attempt to logon to the system using the User ID Guest and pressing return (do not enter a password).	Access denied.		
14.	Attempt to logon to the system using the User ID Guest and enter Guest for the password.	Access denied.		
15.	Attempt to logon to the system using the User ID Administrator and pressing return (do not enter a password).	Access denied.		
16.	Attempt to (or have system administrator) logon to the system using a valid User ID and password.	Logon in Process message window appears.		
17.	Ask the System Administrator if local or centralized virus scanning is used.	If local virus scanning is used skip to question 18.		
18.	If centralized virus scanning is used ask the System Administrator if the virus signatures are kept current on the central scanning system.	Most current version of the virus signatures is being used. Skip to question 21		
19.	If local virus scanning is in use when the desktop appears observe the system tray in the bottom right corner of the desktop to verify that a virus protection software icon is present.	Virus protection software icon is present.		
20.	Have SA show the date of the virus patterns/signatures currently running.	The patterns/signatures should be no more than one month old.		
21.	Right click on the desk top and select Properties	Display Properties window opens.		

Step #	Procedure Description	Expected Results	Actual Results (If different from Expected)	Y/N/P
22.	Select the Screen Saver tab.	<ul style="list-style-type: none"> ◆ A screensaver has been selected. ◆ The Password Protected box is checked. ◆ The Wait time is set to a maximum of 15 minutes. 		
23.	Close Display Properties window.	Display Properties window closes.		
24.	Open Start menu, select Programs and observe the programs listed.	Only approved USDA programs are listed.		
25.	Ask SA if any folders on the workstation are shared with other users.	Depending on the function of the workstation folders may or may not be shared.		
26.	Ask the SA if shared folders are protected from unauthorized access and modification using rights and permissions assignment at a minimum.	Shared software folders are protected from unauthorized access and modification using rights and permissions assignment at a minimum.		
27.	Ask the SA if shared system and security software files are protected from unauthorized access and modification through assignment of permissions and rights.	Shared system and security software files are protected from unauthorized access and modification through assignment of permissions and rights.		
28.	Open Start menu and click on Settings	Settings menu appears.		
29.	Click on Control Panel	Control Panel window opens		
30.	Click on the Control Panel Help menu and select About Windows NT	About Windows NT window opens.		
31.	Verify that Version 4.0 of Windows NT is the current version of the operating system.	The operating system is Windows NT 4.0		
32.	Verify that the current Service Pack is installed.	The current Service Pack has been installed.		
33.	Exit the Help window and exit the Control Panel.	Help and Control Panel windows close.		
34.	Click on the Start menu button in the task bar.	Start menu choices appear.		
35.	Log off the workstation and log back on using the workstation Administrator user ID and password.			

Step #	Procedure Description	Expected Results	Actual Results (If different from Expected)	Y/N/P
36.	Click on the Programs selection.	Program menu appears.		
37.	Select Administrative Tools (Common).	Administrative Tools menu appears.		
38.	Select User Manager.	User Manager window opens.		
39.	Ask SA if domain or local user accounts are used to access workstations.	If local user accounts are used skip to question 38. Test 2 will deal with the configuration of local accounts.		
40.	Observe how many users are listed.	There should only be the local administrator account and the Guest account listed.		
41.	Observe that the Administrator account has been renamed.	Administrator account has been renamed.		
42.	Ask the SA if the Administrator account is used.	Administrator account is not used.		
43.	Ask the SA if users requiring administrative access to workstations have individual accounts with membership in the Administrators Group.	Users requiring administrative access to workstations have individual accounts with membership in the Administrators Group.		
44.	Ask SA if the Guest account has a password.	Guest account has a password.		
45.	Double click the Guest account to view its properties.	Guest account properties dialog window opens.		
46.	Observe that the User Cannot Change Password, Password Never Expires and Account Disabled boxes are checked.	User Cannot Change Password, Password Never Expires and Account Disabled boxes are checked.		
47.	Click on the Groups button in the Guest account properties window and observe what groups the Guest account is a member of.	Guest account is a member of no Groups.		
48.	Close Guest account properties window.	Guest account properties dialog window closes.		
49.	Ask SA if system rights/permissions are assigned based on Group membership of users.	Rights/permissions are assigned based on Group membership of users.		
50.	Ask SA if workstation rights/permissions are assigned to domain groups or	Rights/permissions are assigned to domain groups not individual		

Step #	Procedure Description	Expected Results	Actual Results (If different from Expected)	Y/N/P
	individual users.	users.		
51.	Ask SA if users are assigned to groups based on job function and/or "need to know."	Users are assigned to groups based on job function and/or "need to know."		
52.	Exit the User Manager Menu.	User Manager for Domains Menu closes.		

Comments:

Action Plan:

Test Number: 2	SITE:	DATE:	TIME:
Test Name: NT Workstation Password Policy Configuration (This test is required only if local workstation accounts are used.)			
Resources Required:	Access to the NT Workstation with Administrator Access		
Personnel Required:	NT Workstation Administrator.		
Objectives:	To determine that the NT Password Policies are configured to meet USDA requirements pertaining to Identification and Authentication.		
Procedure Description: (Summary)	Verify that Password Policies are properly configured.		

Detailed Procedures and Results

Step #	Procedure Description	Expected Results	Actual Results (If different from Expected)	Y/N/P
1.	Open the User Manager for Domains from the Start/Programs/Administrative Tools Common menu.			
2.	Click on the Policies menu button at the top of the User Manager for Domains window and select Account.	Account settings screen appears.		
3.	Verify that the account policies match those on the NT Account Policy settings attachment.	The account policies match those on the NT Account Policy Settings attachment.		
4.	Maximum password age is set to 90 days	Maximum password age is set to 90 days		
5.	Minimum password age allows change after 7 days	Minimum password age allows change after 7 days		
6.	Minimum password length is set to 8 characters	Minimum password length is set to 8 characters		
7.	Password Uniqueness is set to remember 5 passwords	Password Uniqueness is set to remember 5 passwords. Note: the Password Uniqueness box will show 3. NT remembers 2 passwords by default and putting 3 in the box will make it a total of 5.		

Step #	Procedure Description	Expected Results	Actual Results (If different from Expected)	Y/N/P
8.	Lock Out is set to lock out after 3 failed login attempts	Lock Out is set to lock out after 3 failed login attempts		
9.	Lock out is set to reset count after 60 minutes	Lock out is set to reset count after 60 minutes		
10.	Lock out duration is set to Forever – Until unlocked by Administrator	Lock out duration is set to Forever – Until unlocked by Administrator		
11.	Click OK.	Account settings screen closes.		

Comments:

Action Plan:

Test Number: 3	SITE:	DATE:	TIME:
Test Name: NT Workstation Registry Settings			
Resources Required:	Administrative access to the NT Workstation.		
Personnel Required:	NT Workstation Administrator.		
Objectives:	To verify that all registry settings in place and correct.		
Procedure Description: (Summary)	Using Regedt32, access the system registry and verify that specific registry keys are correctly configured. <u>WARNING:</u> This test must be done carefully to prevent any damage to the registry. DO NOT ATTEMPT TO EDIT THE REGISTRY!		

Detailed Procedures and Results

Step #	Procedure Description	Expected Results	Actual Results (If different from Expected)	Y/N/P
1.	Click on the Start button in the Task Bar.	Start menu choices appear.		
2.	Click on Run.	Run Dialog window opens.		
3.	Enter Regedt32 in the Run dialog.	Regedt32 starts and the Registry tree appears in the left window.		
4.	Select the HKEY_LOCAL_MACHINE folder.	Hive categories appear.		
5.	Click on Security at the top and select Permissions	Registry Permissions dialog window opens		
6.	Ensure Permissions are correct.	Administrators-Full Control Everybody-Read Only System-Full Control NOTE: The box "Replace Permissions on Existing Subkeys" is NOT checked.		
7.	Exit Permissions dialog window	Permissions dialog window closes		
8.	Select HKEY_LOCAL_MACHINE\Software\Program Groups window, then select the "Security", and "Auditing" menu choices.	Significant changes are audited.		
9.	Select \Microsoft\Windows NT\CurrentVersion\Winlogon. Observe the	The text string within the double quotes is "AUTHORIZED USE		

Step #	Procedure Description	Expected Results	Actual Results (If different from Expected)	Y/N/P
	LegalNoticeCaption in the right side of the window and verify that the text string within the double quotes is "AUTHORIZED USE ONLY."	ONLY."		
10.	Observe the LegalNoticeText in the right side of the window and verify that the text within the double quotes is equivalent to the text in Attachment 1.	The text within the double quotes is equivalent to the text in the Attachment 1.		
11.	Observe the DontDisplayLastUserName entry in the right window and verify that a "1" appears in the double quotes.	A "1" appears in the double quotes.		
12.	Verify that the ShutdownWithoutLogon value is set to 0.	ShutdownWithoutLogon value is set to 0.		
13.	Select \Microsoft\OS/2 Subsystem for NT and ensure that it contains no subkeys.	<p>\Microsoft\OS/2 Subsystem for NT contains no subkeys.</p> <p>Note: These subsystems were not included in the evaluated configuration, and therefore C2-like compliance cannot be achieved unless they are removed.</p>		
14.	Select HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\NotificationPackages has the string passfilt.dll listed.	<p>\NotificationPackages has the string passfilt.dll listed.</p> <p>Note: passfilt.dll forces password complexity.</p>		
15.	Select HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA. The RestrictAnonymous should be present and the value should be set to 1.	<p>RestrictAnonymous has been created and the value is 1.</p> <p>Note: This setting restricts anonymous users from being able to obtain public information about the LSA component of the Windows NT Security Subsystem. The LSA handles aspects of security administration on the local computer, including access and</p>		

Step #	Procedure Description	Expected Results	Actual Results (If different from Expected)	Y/N/P
		permissions.		
16.	Select HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Subsystems and verify there are no entries for Posix and OS/2	There are no entries for Posix and OS/2. Note: These subsystems were not included in the evaluated configuration, and therefore C2-like compliance cannot be achieved unless they are removed.		
17.	Select HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NetBT\Parameters and verify that EnablePortLocking has been added and set to a value of 1.	EnablePortLocking has been added and set to a value of 1. Note: An unprivileged user mode application should not be able to listen to TCP and UDP ports used by Windows NT services, regardless of the cryptographic protection applied to the Windows NT service traffic through the ports.		
18.	Select HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\GraphicsDrivers\DCI\Timeout and verify that the value is set to 0.	Timeout value is set to 0. Note: This prevents direct access to video hardware and memory		
19.	Select HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\ProtectionMode and verify that the value is set to 1.	ProtectionMode value is set to 1. Note: This setting is necessary to further heighten security of the base objects. Among other things, it prevents users from gaining local administrator privileges by way of a dynamic-link library (DLL).		
20.	Select HKEY_LOCAL_MACHINE\SYSTEM\Optional and verify that the folder does not exist or there are no values listed.	There is no Optional folder or no values are listed in the folder.		
21.	Click on the window "HKEY_CLASSES_ROOT". Select "Security", then	Verify that permissions on "HKEY_CLASSES_RO		

Step #	Procedure Description	Expected Results	Actual Results (If different from Expected)	Y/N/P
	"Permissions" from the menu.	OT" and all its subkeys are set to: Administrators - Full Control CREATOR OWNER - Full Control Everyone - Read System - Full Control NOTE: The box "Replace Permissions on Existing Subkeys" is NOT checked.		
22.	Select "HKEY_USERS" and the folder "HKEY_USERS\DEFAULT\UNICODE Program Groups". Select "Security", then "Permissions" from the menu.	Verify that permissions on "HKEY_USERS\DEFAULT\UNICODE Program Groups\[all subkeys]" are set to: Administrators - Full Control Everyone - Read System - Full Control		
23.	Exit Regedt32			

Comments:

Action Plan:

Test Number: 4	SITE:	DATE:	TIME:
Test Name: NT Workstation Audit			
Resources Required:	Access to NT Workstation with Administrator Access		
Personnel Required:	NT Systems Administrator.		
Objectives:	To determine that the NT Workstations are configured to meet USDA requirements pertaining to Auditing.		
Procedure Description: (Summary)	Verify that auditing is turned on, functioning and properly configured. Also, verify that the audit logs are reviewed on a regular basis and backed up on a regular schedule.		

Detailed Procedures and Results

Step #	Procedure Description	Expected Results	Actual Results (If different from Expected)	Y/N/P
1.	Ask the SA if Audit logs are reviewed on a regular basis..	Audit logs are reviewed on a regular basis.		
2.	Ask the SA if the audit logs are backed up according to a routine schedule. Observe back-ups of audit logs.	Audit logs are backed up according to a routine schedule.		
3.	Click on the Start menu button in the task bar.	Start menu choices appear.		
4.	Click on the Programs selection.	Program menu appears.		
5.	Select Administrative Tools (Common).	Administrative Tools menu appears.		
6.	Select User Manager	User Manager window opens.		
7.	Select the Policies menu at the top of the User Manager for Domains window and select Audit.	Audit settings screen appears.		
8.	Verify that the Audit These Events option is selected.	Audit These Events option is selected.		
9.	Verify that all events are selected for Success and Failure except File and Object Access, Use of User Rights, and Process Tracking, which only have only Failure selected. (See Attachment 3)	All events are selected for Success and Failure except File and Object Access, Use of User Rights, and Process Tracking, which only have Failure selected.		
10.	Click OK.	Audit settings screen closes.		
11.	Click the Start button in the task bar.	Start menu choices appear.		
12.	Select Programs.	Programs menu appears.		
13.	Select Administrative Tools	Administrative Tools		

Step #	Procedure Description	Expected Results	Actual Results (If different from Expected)	Y/N/P
	(Common).	menu appears.		
14.	Select Event Viewer.	Event Viewer window opens.		
15.	At the top of the Event Viewer window click on the Log menu selection.	Log menu appears.		
16.	Select the System Log.	System log appears in window.		
17.	Click on the log menu again and select Log Settings.	System log settings dialogue appears.		
18.	Verify that "Do Not Overwrite" box is checked.	"Do Not Overwrite" box is checked.		
19.	Click OK on Log Settings Dialogue.	Log Settings Dialogue window closes.		
20.	At the top of the Event Viewer window click on the Log menu selection.	Log menu appears.		
21.	Select the Application Log.	Application log appears in window.		
22.	Click on the log menu again and select Log Settings.	Application log settings dialogue appears.		
23.	Verify that "Do Not Overwrite" box is checked.	"Do Not Overwrite" box is checked.		
24.	Click OK on Log Settings Dialogue.	Log Settings Dialogue window closes.		
25.	At the top of the Event Viewer window click on the Log menu selection.	Log menu appears.		
26.	Select the Security Log.	Security log appears in window.		
27.	Click on the log menu again and select Log Settings.	Security log settings dialogue appears.		
28.	Verify that "Do Not Overwrite" box is checked.	"Do Not Overwrite" box is checked.		
29.	Click OK on Log Settings Dialogue.	Log Settings Dialogue window closes.		
30.	Close Event Viewer window.	Event Viewer window closes.		

Comments:

Action Plan:

Test Number: 5	SITE:	DATE:	TIME:
Test Name: NT Workstation System Backups			
Resources Required:	Access to an NT Workstation with Administrator Access		
Personnel Required:	NT Workstation Administrator.		
Objectives:	To ensure that NT Workstations operating systems and applications are backed up on a timely basis and that backup procedures are being performed.		
Procedure Description: (Summary)	Examine backup scheduler program and log files to determine that backups are conducted on a timely basis. Review NT Workstation backup procedures and determine that procedures are being performed.		

Step #	Procedure Description	Expected Results	Actual Results (If different from Expected)	Y/N/P
1.	Log onto workstation as Administrator.	Successful log-on.		
2.	Review backup scheduler programs and log files to determine that backups are conducted on a timely basis.	Backups are conducted on a timely basis.		
3.	Ask Administrator for workstation backup procedures document and ask if the procedures are being followed.	Workstation backup procedures documentation is available and procedures are being performed as required.		
4.	Ask SA if copies of backups are stored off-site, in a secure environment on a regular basis.	Copies of backups are stored off-site, in a secure environment on a regular basis.		

Comments:

Action Plan:

ATTACHMENT 1

Legal Notice Text string:

UNAUTHORIZED ACCESS TO THIS UNITED STATES GOVERNMENT COMPUTER SYSTEM AND SOFTWARE IS PROHIBITED BY PUBLIC LAW 99-474, TITLE 18, UNITED STATES CODE. PUBLIC LAW 99-474 AND CHAPTER XXI, SECTION 1030 STATES THAT...

Whoever knowingly, or intentionally accesses a computer without authorization or exceeds authorized access, and by means of such conduct, obtains, alters, damages, destroys, or discloses information, or prevents authorized use of (data or a computer owned by or operated for) the Government of the United States, shall be punished by a fine under this title or imprisonment for not more than 10 years, or both.

All activities on this system may be recorded and monitored. Individuals using this system expressly consent to such monitoring. Evidence of possible misconduct or abuse may be provided to appropriate officials.

REPORT UNAUTHORIZED USE TO AN INFORMATION SYSTEMS SECURITY OFFICER

ATTACHMENT 2**NT Domain Account Policy Settings**

Account Policy [X]

Computer: BULLB

Password Restrictions

Maximum Password Age

☐ Password Never Expires

☒ Expires In Days

Minimum Password Age

☐ Allow Changes Immediately

☒ Allow Changes In Days

Minimum Password Length

☐ Permit Blank Password

☒ At Least Characters

Password Uniqueness

☐ Do Not Keep Password History

☒ Remember Passwords

☐ No account lockout

☒ Account lockout

Lockout after bad logon attempts

Reset count after minutes

Lockout Duration

☒ Foreever (until admin unlocks)

☐ Duration minutes

☒ Users must log on in order to change password

OK Cancel Help

ATTACHMENT 3

Audit Policy Settings:

